ON AN ARITHMETICAL FUNCTION RELATED TO EULER'S TOTIENT AND THE DISCRIMINATOR

Pieter Moree
Freesiastraat 13, 2651 XL Berkel en Rodenrijs, The Netherlands

Hans Roskam
Wilhelminapark 4, 2342 AG Oegstgeest, The Netherlands
(Submitted January 1994)

1. INTRODUCTION

The discriminator, $D(j, n)$, is defined to be the smallest positive integer k for which the first n j^{th} powers are distinct modulo k. It was introduced by Arnold, Benkoski, and McCabe [1] in order to determine the complexity of an algorithm they had developed. Results on the discriminator can be found in [1, 3, 4, 12, 13, 16, 17]. We show that, under certain conditions, the discriminator takes on values that are also assumed by the function $E(n) := \min\{k : n|\varphi(k)\}$. Here φ denotes Euler's totient. We call E the *Euler minimum function*. The sequence $\{a_k\}_{k=1}^{\infty}$, with $a_k = \operatorname{lcm}(\varphi(1), \ldots, \varphi(k))$ is used to link the discriminator and the Euler minimum function. As an application we show that, for several values of n and primes p, there exist unbounded sequences $\{j_k\}_{k=1}^{\infty}$ and $\{e_k\}_{k=1}^{\infty}$, such that $D(j_k, n) = p^{e_k}$ for every natural number k. The prime powers p^{e_k} are exceptional values of the discriminator, since it is known that $D(j, n)$ is squarefree for every fixed $j > 1$ and every n large enough [4]. For example, if $j > 1$ and j is odd, one has, for every n sufficiently large, $D(j, n) = \min\{k \geq n | \gcd(j, \varphi(k)) = 1 \text{ and } k \text{ is squarefree}\}$. In the literature so far only the case where j is fixed has been considered. In this paper we focus on the case where n is fixed. The behavior of $D(j, n)$ turns out to be very different in these cases. (For a table of values of the discriminator, see [17].)

Since we think that the Euler minimum function and the sequence $\{a_k\}_{k=1}^{\infty}$ are of interest in themselves, we also prove some results on them which are possibly not related to discriminators.

2. RESULTS ON THE EULER MINIMUM FUNCTION

There seems to be no literature on $E(n)$. The related set $\{k : n|\varphi(k)\}$, however, does occur in the literature. It is denoted by C_n [we will use the notation $C(n)$] and occurs in a series of papers on the equidistribution of the integers coprime with n ("the totatives") in intervals of length n/k written in the 1950s [6, 7, 10, 11]. In particular, it is shown there that $A(n) = C(n)$ if and only if n is prime, where $A(n)$ is the set $\{k \in \mathbb{N} : n^2 | k$ or there exists a p with $p \equiv 1 \pmod{n}$ and $p|k\}$. A result on $C(n)$ of a different kind (and time) is that of Dressler [5], who proved that the set $\mathbb{N} \setminus C(n)$ has natural density zero for every n.

Recall that if $\prod p_i^{\alpha_i}$ is the canonical prime factorization of n, then $\varphi(n) = \prod p_i^{\alpha_i - 1}(p_i - 1)$. So, in particular, $n|\varphi(n^2)$ and, therefore, $E(n) \leq n^2$, and so $E(n)$ exists. In the proofs, we repeatedly use the following simple principle to show that a certain number does not equal the $E(n)$: we exhibit a smaller number in the collection $C(n)$. We study only the case where n equals a prime power.

The symbol p is used exclusively for primes.

Theorem 1: Let q be a prime. Let m be the smallest squarefree number of the form $\prod_{i=1}^{k}(1+a_i q^{e_i})$ with $1+a_i q^{e_i}$ prime for $i=1,\ldots,k$ and $\sum_{i=1}^{k} e_i = n$. Then

$$E(q^n) = \min\{m, q^{n+1}\}.$$

In case $E(q^n) = m$, we have

$$\prod_{i=1}^{k} a_i < q \quad \text{and} \quad \prod_{i=1}^{k} a_i = \varphi(m)/q^n.$$

Remark: By Dirichlet's theorem on arithmetical progressions, m exists.

Proof: Assume that $p \neq q$ and $p \mid E(q^n)$. If $p^2 \mid E(q^n)$, then the integer $E(q^n)/p$ is also in $C(q^n)$. Since this contradicts the definition of $E(q^n)$, it follows that $p^2 \nmid E(q^n)$. Since the integer $E(q^n)/p$ is not in $C(q^n)$, we have $p \equiv 1 \pmod{q}$. Therefore, $p = 1 + aq^e$ for some positive integers a and e. Also, if $q \mid E(q^n)$, then the integer $E(q^n)q^e/p$, which is less than $E(q^n)$, is in $C(q^n)$. Put $g = \mathrm{ord}_q(\varphi(E(q^n)))$. Obviously, $g \geq n$. If $g > n$, then the integer $E(q^n)q^e/p$, which is less than $E(q^n)$, is in $C(q^n)$. This contradiction shows that $g = n$. Up to this point we have shown that $E(q^n)$ is a squarefree number of the form $\prod_{i=1}^{k}(1+a_i q^{e_i})$ with $1+a_i q^{e_i}$ prime for $i=1$, ..., k and $\sum_{i=1}^{k} e_i = n$. Clearly, $E(q^n)$ has to be the smallest number of this form, that is, $E(q^n) = m$. In the remaining case where $E(q^n)$ does not have a prime divisor p with $p \neq q$, we have $E(q^n) = q^{n+1}$. It follows that $E(q^n) = \min\{m, q^{n+1}\}$. In the case $m < q^{n+1}$, we have $\varphi(m) = \prod_{i=1}^{k} a_i q^{e_i} = q^n \prod_{i=1}^{k} a_i < m < q^{n+1}$ and the remaining part of the assertion follows. □

In order to compute $E(q^n)$, the following variant of Theorem 1 is more convenient to work with. We denote by $S(q)$ the set of squarefree numbers composed of only primes p satisfying $p \equiv 1 \pmod{q}$. For convenience, we define the minimum of the empty set to be ∞.

Theorem 1': $E(q^n) = \min\{m, q^{n+1}\}$, where $m = \min\{s \in S(q) : q^n \text{ divides } \varphi(s)/q^n < q\}$.

For given positive integers a and d with $\gcd(a,d)=1$, we denote by $p(d,a)$ the smallest prime p satisfying $p \equiv a \pmod{d}$ and more in general by $p_i(d,a)$, $i \geq 2$, the i^{th} smallest such prime. We denote by $\omega(n)$ the number of distinct prime factors of n.

Corollary 1:

(i) The largest prime divisor of $\varphi(E(q^n))$ is q.
(ii) The smallest prime divisor of $E(q^n)$ is not less than q.
(iii) If q is odd, then $\omega(E(q^n)) < \min\{n+1, \log q/\log 2\}$.
(iv) $E(q) = \min\{q^2, p(q,1)\}$.
(v) $E(q^2) = \min\{q^3, p(q^2,1), p(q,1)p_2(q,1)\}$.

Theorem 1 and in particular parts (iv) and (v) of Corollary 1 show that the behavior of the Euler minimum function is intimately tied up with the distribution of prime numbers. Theorem 1 gives rise to questions on the behavior of $p(q,1)$ and, if we delve deeper, on $p_i(q,1)$ for $i \geq 2$. Corollary 1(v), for example, gives rise to the following question: Is it true that infinitely often $p(q,1)p_2(q,1) < p(q^2,1)$? Unfortunately, problems involving $p(d,a)$ are generally very difficult (see, e.g., [14, p. 217] for an overview). However, there is a guiding principle in these difficult matters: probabilistic reasoning. The basic assumptions made in probabilistic reasoning are that the probability that n is a prime is about $1/\log n$ and that the events n is a prime and m is a prime are independent. Using probabilistic reasoning, we arrive, for example, at the conjecture that $p(q,1) < q^2$ for every sufficiently large prime q. Indeed, this conjecture was made by several mathematicians (see, e.g., [9] [15]). Very recently, Bach and Sorenson [2] proved that $p(q,1) < 2(q\log q)^2$, assuming the Extended Riemann Hypothesis holds true. By Corollary 1(iv), the conjecture is equivalent to $E(q) = p(q,1)$ for every prime q large enough. Unconditionally, we can only prove the following result.

Lemma 1: $|\{q \le x : E(q) = p(q,1)\}| \gg x^{.6687}/\log x$.

Proof: Put $A_a(x,\delta) = |\{p : a+2 \le p \le x,\ P(p-a) \ge x^{\delta}\}|$, where $P(n)$ denotes the greatest prime divisor function. Put $\delta = .6687$. Then by Théorème 1 of Fouvry [8]. $A_a(x,\delta) \gg x/\log x$, where the implied constant depends only on a. Let p be a prime contributing to $A_a(x,\delta)$. Put $P(p-a) = q$. Then $p(q,a) \le p \le x \le q^{1/\delta}$. Since there are at most $x^{1-\delta}$ primes p such that $P(p-a) = q$ and $q \ge x^{\delta}$ (a fixed), it follows that

$$|\{q \le x : p(q,a) \le q^{1/\delta}\}| \ge \frac{A_a(x,\delta)}{x^{1-\delta}} \gg x^{\delta}/\log x.$$

In particular, we have $|\{q \le x : p(q,1) < q^2\}| \gg x^{.6687}/\log x$. □

Remark: Let a be an arbitrary fixed positive integer. The result implicit in the proof of Lemma 1 that

$$|\{q \le x : p(q,a) < q^{1.496}\}| \gg x^{.6687}/\log x,$$

supersedes the record result of Motohashi mentioned in *The Book of Prime Number Records* [14, p. 218], who proved in 1970 that $|\{q \le x : p(q,a) < q^{1.6378}\}|$ tends to infinity with x.

The following lemma is a straightforward consequence of Theorem 1.

Lemma 2:

(i) $E(p^a) \ne E(q^b)$ if $p \ne q$.

(ii) $E(p^a) \ne E(p^b)$ if $a \ne b$.

Proof:

(i) If $E(p^a) = E(q^b)$, then $P(\varphi(E(p^a))) = P(\varphi(E(q^b)))$. If $p \ne q$, this is impossible by Corollary 1(i).

(ii) Since, by Theorem 1, $p^a \| \varphi(E(p^a))$ and $p^b \| \varphi(E(p^b))$, clearly $E(p^a) \ne E(p^b)$ if $a \ne b$. □

If $q = 2$, Theorem 1 can be improved. For $j \ge 0$ put $\mathcal{F}_j = 1 + 2^{2^j}$. The primes of this form are called *Fermat primes*. Let I be the set of i such that $\mathcal{F}_i$ is prime. Notice that 0, 1, 2, 3, and 4 are in I. These numbers correspond with the primes 3, 5, 17, 257 and 65537. These primes are the only known Fermat primes.

Lemma 3: Let $\sum_{j\in J} 2^j$ be the representation to the base 2 of n. Then

$$E(2^n) = \begin{cases} \prod_{j\in J} \mathcal{F}_j & \text{if } J \text{ is a subset of } I; \\ 2^{n+1} & \text{otherwise.} \end{cases}$$

Proof: Notice that the number m (in the notation of Theorem 1′) equals $\min\{s \in S(2): \varphi(s) = 2^n\}$. The prime factors of m must all be Fermat primes (for a number of the form $1+2^b$ to be prime, it is necessary that b is a power of two). On using the uniqueness of the representation to the base 2, it follows that $m = \prod_{j \in J} \mathcal{F}_j$ if J is a subset of I and ∞ otherwise. Multiplying out $\prod_{j \in J}(2^{2^j}+1)$ gives a sum of powers of 2 with unequal exponents and largest exponent n. So $\prod_{j \in J} \mathcal{F}_j < 2^{n+1}$ (using the uniqueness of the representation to the base 2 again). The lemma then follows from Theorem 1′. □

Example: $E(2^{31}) = 4294967295$.

Corollary: If there are only finitely many Fermat primes, then $E(2^a) = 2^{a+1}$ for every sufficiently large a.

Remark: The prime 2 seems to be the only one for which such an explicit result can be derived. This is in agreement with the saying of H. Zassenhaus that two is the oddest of primes.

The next lemma demonstrates that, for some odd primes, Theorem 1′ can also be sharpened, although to a lesser extent.

Lemma 4: $E(q^n) = \min\{q^{n+1}, p(q^n, 1)\}$ for $q = 3, 7, 13$, and 31. $E(q^n) = \min\{q^{n+1}, p(q^n, 1)\}$ if n is odd for $q = 5$ and 19.

Proof: We only work out the case where $q = 19$, the other cases being similar. Notice that $3 | 1+2.19^a$, so $1+2.19^a$ is not a prime. Then $\{s \in S(19): 19^n | \varphi(s), \varphi(s) < 19^{n+1}$ and $\omega(s) \geq 2\} = \{(1+4.19^a)(1+4.19^b): a+b = n$ and both $1+4.19^a$ and $1+4.19^b$ are prime$\}$. Now, since n is odd, we can assume without loss of generality that a is even. But then $5 | 1+4.19^a$, so this collection is empty. Therefore, by Theorem 1′, we find that $E(19^n) = \min\{19^{n+1}, p(19^n, 1)\}$. □

In the next section it is shown that primes p such that $E(p^n) = p^{n+1}$ for infinitely many n are related to special values of this discriminator. Let E denote the collection of primes having this property.

Lemma 5: $2 \in E$.

Proof: Since $F_5 = 641 \cdot 6700417$ is composite (Euler), it follows from Lemma 3 that $E(2^n) = 2^{n+1}$ for every n that has 2^5 in its representation to the base 2. Since there are obviously infinitely many such n, the lemma follows. □

Lemma 6: Let q be an odd prime. Suppose there are integers a, d, and n_0 such that $E(q^n) = \min\{q^{n+1}, p(q^n, 1)\}$ for every $n \geq n_0$ and $n \equiv a \pmod{d}$. Then q is in E.

Proof: Let k be an arbitrary integer such that $k \geq n_0$ and $k \equiv a \pmod{d}$. For every j in $\{1, \ldots, (q-1)/2\}$, choose some prime divisor p_j of $1+2jq^k$. Notice that $\gcd(p_j, q) = 1$. Then, by Fermat's little theorem, $p_j | 1+2jq^{k+m(p_j-1)}$ for every j in $\{1, \ldots, (q-1)/2\}$, so $1+2jq^{k+m(p_j-1)}$ is composite for every m in $\mathbb{N}$ and j in $\{1, \ldots, (q-1)/2\}$. Put $\ell = \operatorname{lcm}(p_1 - 1, \ldots, p_{(q-1)/2} - 1)$. Then $1+2jq^{k+m\ell d}$ is composite for every m in $\mathbb{N}$ and j in $\{1, \ldots, (q-1)/2\}$. Since $k+m\ell d \equiv a \pmod{d}$ and $k+m\ell d \geq n_0$, it follows from the hypothesis of the lemma that $E(q^{k+m\ell d}) = q^{k+1+m\ell d}$ for every m in $\mathbb{N}$; therefore, q is in E. □

Finally, using Lemmas 4, 5, and 6, we find

Lemma 7: $\{2,3,5,7,13,19,31\} \subseteq E$.

We conjecture that in fact every prime is in E and challenge the reader to prove this or, at least, to exhibit other primes in E.

3. THE LOWEST COMMON MULTIPLE OF THE SUCCESSIVE TOTIENTS

In this section we study the sequence $\{a_k\}_{k=1}^{\infty}$, with $a_k = \operatorname{lcm}(\varphi(1), \ldots, \varphi(k))$; in plain English, a_k is the lowest common multiple of the first k totients. In the next paragraph it will transpire that this strange sequence provides a link between discriminators and the Euler minimum function. The purpose of this section is to give the reader some feeling for the behavior of this sequence.

Put $c_k = a_k / a_{k-1}$ for $k \geq 2$. We say k (≥ 2) is a *jumping point* if c_k exceeds one.

Lemma 8: The number k is a jumping point if and only if $k = E(p^r)$ for some prime p and exponent $r > 1$.

Proof: If k is a jumping point, then there is a prime p such that $p | c_k$. Put $r = \operatorname{ord}_p(\varphi(k))$. Then $p^r \nmid \varphi(\ell)$ for every $\ell < k$ (otherwise $p \neq c_k$), so $k = E(p^r)$. On the other hand, if $k = E(p^r)$ for some prime p and exponent r, then $c_k \geq p$, so k is a jumping point. □

Lemma 9: For $k \geq 2$, c_k is a prime or equals 1.

Proof: If $c_k > 1$, then $k = E(p^r)$ by the previous lemma. Now p is the only prime dividing c_k because if another prime, say q, would divide c_k, then it would follow that $E(p^r) = E(q^a)$, where $q^a \| \varphi(k)$. By Lemma 2(i), this is impossible. If $p^2 | c_k$, then $p^{r-1} \nmid \varphi(\ell)$ for every $\ell < k$, and it follows that $E(p^{r-1}) = E(p^r)$. By Lemma 2(ii), this is impossible. □

The following lemma gives an idea of the growth of the sequence $\{a_k\}_{k=1}^{\infty}$ as k tends to infinity. A trivial lower bound for a_k is given by $\exp(c\sqrt{k})$ for some $c > 0$. To see this, note that $\prod_{p \leq \sqrt{k}} p$ divides a_k (since $p | \varphi(p^2)$). On using the result $\sum_{p \leq x} \log p \sim x$ of prime number theory, the bound is easily established.

Lemma 10: Let ε be an arbitrary fixed positive real number. Then

$$\exp(k^{.6687}) \ll a_k \ll \exp((1+\varepsilon)k).$$

Proof: Recall that $\Lambda(n)$, the Von Mangoldt function, is defined by $\log p$ if n is of the form p^k, and 0 otherwise. Notice that

$$\log(a_k) \leq \log(\operatorname{lcm}(1, \ldots, k)) = \sum_{n \leq k} \Lambda(n) \leq (1+\varepsilon)k$$

for every k sufficiently large. The latter estimate follows from the well-known result

$$\sum_{n \leq x} \Lambda(n) \sim x$$

of prime number theory. This gives the upper bound.

The primes contributing to $A_1(k,\delta)$ (cf. the proof of Lemma 1) yield $\gg k^{\delta}/\log k$ distinct primes not less than k^{δ} that occur as prime factors of numbers of the form $p-1$ with p not exceeding k. The product of these primes is a divisor of a_k exceeding $\exp(ck^{\delta})$ for some $c>0$ and all $k\geq 1$. □

Remark: In case $A_a(x,\delta)\gg x/\log x$ holds for a number larger than .6687, this automatically gives rise to a corresponding improvement in Lemmas 1 and 10.

4. THE EULER MINIMUM FUNCTION AND THE DISCRIMINATOR

For $n=1, 2$, and 3, the behavior of the discriminator is not very interesting; it is easy to show that $D(j,1)=1$, $D(j,2)=2$, $D(2j-1,3)=3$, and $D(2j,3)=6$ for every j in $\mathbb{N}$. From now on we assume that n is an arbitrary fixed integer ≥ 4. We establish a connection between the Euler minimum function and discriminators.

First, we prove a lemma ("the push-up lemma") that can be used, given an arbitrary k, to find a j such that $D(j,n)\geq k$. In the proof, the following result on $e(k)$, the maximum of the exponents in the canonical prime factorization of k, is needed.

Lemma 11: $e(k)\leq\varphi(k)$.

Proof: For $k=1$ there is nothing to prove. If $k>1$, there is a prime p and an exponent $e(k)\geq 1$ such that $p^{e(k)}\| k$. Then $e(k)\leq 2^{e(k)-1}\leq p^{e(k)-1}(p-1)\leq\varphi(k)$. □

For convenience, we call a pair of integers r, s with $1<r\leq s\leq n$ an *n-pair*. When both r and s are coprime with k, the n-pair (r, s) is said to be coprime with k.

Lemma 12 ("push-up lemma"): For $n\geq 4$ and arbitrary k, we have $D(\varphi(k),n)\neq k$.

Proof: It suffices to exhibit an n-pair (r, s) such that $r^{\varphi(k)}\equiv s^{\varphi(k)}$ (mod k). We show that (2, 4) meets this requirement. Let $f=\mathrm{ord}_2 k$, then $2^{\varphi(k)}\equiv 1$ (mod $k/2^f$). By Lemma 11 and the definition of $e(k)$, it follows that $f\leq e(k)\leq\varphi(k)$, so $2^{\varphi(k)}\equiv 4^{\varphi(k)}$ (mod k). □

We will now use the push-up lemma to prove that there is a connection between the Euler minimum function and discriminators.

Theorem 2: If $n\geq 4$ and $p>n/2$ and p^a is a power of p for which $E(p^{\alpha})\geq n$, and if $p^{\alpha}\,|\,\mathrm{ord}_{E(p^{\alpha})}(r/s)$ for every n-pair (r, s) coprime with $E(p^{\alpha})$, then $D(a_{e(p^{\alpha})-1},n)=E(p^{\alpha})$.

Proof: Put $k=E(p^{\alpha})$. By the push-up lemma $D(a_{k-1},n)\geq k$. We claim that $D(a_{k-1},n)=k$. Put $j=a_{k-1}$. Notice that it suffices to show that there does not exist an n-pair (r, s) such that $r^j\equiv s^j$ (mod k). To this end, assume that such integers do exist. Since the smallest prime divisor of k is not less than p by Corollary 1(ii), it follows from $p>n/2$ that at least one of gcd(r, k) and gcd(s, k) equals one, but then both gcd(r, k) and gcd(s, k) equal one [so the n-pair (r, s) is coprime with k]; thus, $(r/s)^j\equiv 1$ (mod k) and, therefore, j is a multiple of $\mathrm{ord}_{E(p^{\alpha})}(r/s)$. Since this order is divisible by p^{α} by assumption, it follows by the definition of a_{k-1} that there is an $\ell<k$ [$=E(p^a)$], so the theorem is proved. □

Corollary: Suppose that n, p, and α satisfy the hypothesis of Theorem 2. Then $E(p^\alpha)$ is in $D(\mathbb{N}, m)$ for m in $\{4, \ldots, n\}$.

Remark: In Table 1, some triples $(k, E(k), n_{\max})$ are recorded with k of the form p^α, with p^α and $n_{\max}$ satisfying the hypothesis of Theorem 2. Furthermore, $n_{\max}$ is the smallest integer ≥ 4 such that p^α and $n_{\max}+1$ do not satisfy the hypothesis of Theorem 2.

TABLE 1. Numerical Material Related to Theorem 2

k	$E(k)$	$n_{\max}$	k	$E(k)$	$n_{\max}$	k	$E(k)$	$n_{\max}$	k	$E(k)$	$n_{\max}$
7	29	4	13	53	6	17	103	8	19	191	4
25	101	4	27	81	4	31	311	5	37	149	9
43	173	12	47	283	12	49	197	5	59	709	18
61	367	12	67	269	12	71	569	14	73	293	16
79	317	13	97	389	16	101	607	22	103	619	21
107	643	17	127	509	21	137	823	18	139	557	18
151	907	25	163	653	21	169	677	9	193	773	21

If $(E(k), n_{\max})$ is a pair in the table, then $E(k) \in D(\mathbb{N}, m)$ for every $m \in \{4, \ldots, n_{\max}\}$.

The next theorem can be regarded as a special case of Theorem 2. It shows that the hypothesis of Theorem 2 can be weakened at the cost of generality.

Theorem 3: Let $n \geq 4$ and $p \geq n$ be such that $2p+1$ is prime. Then $D(a_{2p}, n) = 2p+1$.

Proof: Notice that $\{p : 2p+1 \text{ is prime, } p \geq 3\} = \{p : E(p) = 2p+1\}$. Let (r, s) be an n-pair. Since $2p+1 \nmid r-s$ and $2p+1 \nmid r+s, r^2 \not\equiv s^2 \pmod{2p+1}$. Therefore, $p \mid \operatorname{ord}_{E(p)}(r/s)$ for every n-pair (r, s) and so the result follows from Theorem 2. □

Remark: The primes in the set $\{p : 2p+1 \text{ is prime, } p \geq 3\}$ are called *Sophie Germain* primes. They were first considered in the study of Fermat's last theorem.

From the results in [4], it follows that $D(j, n)$ is squarefree for every fixed $j \geq 2$ and every n sufficiently large. We proceed to show that there are values of n and primes p such that p^e is in $D(\mathbb{N}, n)$ for infinitely many n. For convenience, we call these primes *n-discriminator primes*. Notice that p^e with e large is far from being squarefree. So, if p^e is in $D(\mathbb{N}, n)$ for some large e, the number p^e can be regarded as an exceptional value of the discriminator.

Lemma 13: Suppose p is odd. If $a^g \equiv 1 + kp \pmod{p^2}$, then $a^{p^{m-1}g} \equiv 1 + kp^m \pmod{p^{1+m}}$.

Proof: The proof is left as an exercise for the interested reader. □

When $\gcd(r, p) = 1$, we have $r^{p-1} = 1 + q_r(p)p$, with $q_r(p)$ an integer. This integer is called the *Fermat quotient* of p, with base r.

Theorem 4: If $n \geq 4, p \in E, p > n/2, q_2(p) \not\equiv 0 \pmod p$ and $q_r(p) \not\equiv q_s(p) \pmod p$ for every n-pair (r, s) coprime with p, then p is an n-discriminator prime.

Proof: By the hypothesis on p and Lemma 13, it follows that $r^{p^{e-1}(p-1)} \not\equiv s^{p^{e-1}(p-1)} \pmod{p^{e+1}}$ for every positive integer e and for every n-pair (r, s) coprime with p. Since $p > n/2$, it even holds true for every n-pair (r, s). Notice that this incongruence implies $p^e \mid \mathrm{ord}_{p^{e+1}}(r/s)$ for every $e \geq 1$. Since p is in E, there are infinitely many exponents f such that $E(p^f) = p^{f+1}$. Then, for all sufficiently large of these f, there exists a j_f such that $D(j_f, n) = p^{f+1}$, by Theorem 2. So p is an n-discriminator prime. □

Corollary: If p is an n-discriminator prime satisfying the hypothesis of Theorem 4, p is an m-discriminator prime for m in $\{4, \ldots, n\}$.

Remark: Fix some p. Suppose there is an n such that n and p satisfy the hypothesis of Theorem 4. Then define $n_{\max}$ to be the largest n such that $n_{\max}$ and p satisfy the hypothesis of Theorem 4. Notice that $n_{\max}$ exists ($n_{\max} < 2p$). The entries in Table 2 result, after some easy computations, on using Theorem 4 and Lemma 4.

TABLE 2. Numerical Material Related to Theorem 4

n	n-Discriminator Primes
4	3, 7, 13, 19, 31
5	13, 19, 31
6	13, 19, 31
7	13, 19, 31
8	19, 31
9	19, 31
10	19, 31
11	31
12	31
13	31
14	31

If p is in the row headed n, then there are infinitely many e such that $p^e \in D(\mathbb{N}, n)$.

Our final theorem shows that the condition $p > n/2$ in Theorem 4 is necessary for p to be an n-discriminator prime.

Theorem 5: If $p \leq n/2$, then p is not an n-discriminator prime.

To prove this, we need some preparatory lemmas. They give upper bounds for $D(j, n)$ that, with harder work, are not too difficult to improve upon. For our purposes, the given bounds will do, however.

Let $p_1, p_2, p_3, \ldots$ denote the sequence of rational primes and $[x]$ the greatest integer $\leq x$.

Lemma 14: $D(j, n) \leq p_{[jn^2 \log n/\log 4]+1}$ for all positive integers j and n.

Proof: For $n = 1$ the assertion is obviously correct. So assume $n > 1$. Let Diff(j, n) denote the set $\{s^j - r^j \mid 1 \leq r < s \leq n\}$. If p is a prime such that p divides none of the members of Diff(j, n), then $1^j, \ldots, n^j$ are pairwise incongruent modulo p and so $D(j, n) \leq p$. Since a number m has at most $[\log m/\log 2]$ different prime factors, the numbers in the set Diff(j, n) contain at most $[jn^2 \log n/\log 4]$ different prime factors. Therefore, there is a prime $q \leq p_{[jn^2 \log n/\log 4]+1}$ such that $1^j, \ldots, n^j$ are pairwise incongruent modulo q. Thus, $D(j, n) \leq q \leq p_{[jn^2 \log n/\log 4]+1}$. □

Lemma 15: $D(j,n) \ll_n j\log(j+1)$.

Proof: The proof is immediate from Lemma 14 and the estimate $p_n = O(n\log n)$, which follows from the Prime Number Theorem. □

Proof of Theorem 5: Suppose $p \le n/2$. Now in case $D(j,n) = p^e$ for some integers j and e, it follows that $e > j$, for if $e \le j$, then $p^j \equiv (2p)^j \pmod{p^e}$. So if p is an n-discriminator prime, there exist infinitely many j such that $D(j,n) \ge p^{j+1}$. However, this contradicts Lemma 15. □

ACKNOWLEDGMENT

We thank Prof. R. Tijdeman for proofreading early versions of this paper and Prof. M. N. Huxley for suggesting a method for obtaining a nontrivial lower bound for $\operatorname{lcm}(\varphi(1), \ldots, \varphi(k))$ as a function of k.

REFERENCES

1. L. K. Arnold, S. J. Benkoski, & B. J. McCabe. "The Discriminator (A Simple Application of Bertrand's Postulate)." *Amer. Math. Monthly* **92** (1985):275-77.
2. E. Bach & J. Sorenson. "Explicit Bounds for Primes in Residue Classes." To appear in *Math. Comp.*
3. M. Barcau. "A Sharp Estimate of the Discriminator." *Nieuw Arch. Wisk.* **6** (1988):247-50.
4. P. S. Bremser, P. Schumer, & L. C. Washington. "A Note on the Incongruence of Consecutive Integers to a Fixed Power." *J. Number Theory* **35** (1990):105-08.
5. R. E. Dressler. "A Property of the φ and σ_j Functions." *Compositio Math.* **31** (1975):115-18.
6. P. Erdös. "Some Remarks on a Paper of McCarthy." *Canad. Math. Bull.* **1** (1958):71-75.
7. P. Erdös. "Remarks and Corrections to My Paper 'Some Remarks on a Paper of McCarthy.'" *Canad. Math. Bull.* **3** (1960):127-29.
8. E. Fouvry. "Théorème de Brun-Titchmarsh: Application au Théorème de Fermat." *Invent. Math.* **79** (1985):383-407.
9. H. J. Kanold. "Elementare Bertrachtungen zur Primzahltheorie." *Arch. Math.* **14** (1963): 147-51.
10. D. H. Lehmer. "The Distribution of Totatives." *Canad. J. Math.* **7** (1955):347-57.
11. P. J. McCarthy. "Note on the Distribution of Totatives." *Amer. Math. Monthly* **64** (1957): 585-86.
12. P. Moree. "On the Incongruence of Consecutive Polynomial Values." Preprint.
13. P. Moree & G. L. Mullen. "Dickson Polynomial Discriminators." Preprint.
14. P. Ribenboim. *The Book of Prime Number Records.* New York: Springer-Verlag, 1989 (2nd ed., 1990).
15. A. Schinzel & W. Sierpinski. "Sur certain hypothèses concernant les nombres premiers." *Acta Arith.* **4** (1958):185-208.
16. P. Schumer. "On the Incongruence of Consecutive Cubes." *Math. Student* **58** (1990):42-48.
17. P. Schumer & J. Steinig. "On the Incongruence of Consecutive Fourth Powers." *Elem. Math.* **43** (1988):145-49.

AMS Classification Numbers: 11A25, 11A07

❖❖❖